REMARKS

In accordance with the foregoing, claim 20 is amended to clarify the claimed subject matter. No new matter is added. Claims 5 and 25 were previously cancelled. Claims 1-4, 6-24, and 26-41 are pending and under consideration.

CLAIM REJECTIONS UNDER 35 USC § 112

Claim 20 is rejected under 35 U.S.C. 112, first paragraph, as not being enabled. The claim is amended herewith to clarify the claimed subject matter. Applicant believes that amended claim 20 is supported by the originally filed application. In view of the claim amendments, Applicants respectfully request withdrawal of this rejection.

CLAIM REJECTIONS UNDER 35 U.S.C. §102

Claims 1-4, 6-24, and 26-41 are rejected under 35 U.S.C. §102(b) as allegedly being anticipated by U.S. Patent No. 5,991,399 to Graunke et al. (hereinafter "Graunke"). Applicants traverse the rejection as argued below.

Independent claim 1 is directed to an information reproducing apparatus having a hardware secure module, a memory, a falsification checking unit, and a processor.

Independent claim 1 patentably distinguishes over the prior art at least by reciting "a **hardware secure module having a tamper resistant module structure** and storing information related to secure software" (emphasis added).

Graunke discloses a method for secure distribution of a private key usable to decrypt encrypted digital content, to a user's application program (such as, a DVD player or CD-ROM player) after verification of the decryption program's integrity and authenticity (see Graunke's title and abstract). Thus, Graunke relates to protection of digital content in digital communication, and, more specifically, to dynamically and securely distributing a private key over a network to enable only a trusted player to decrypt encrypted digital content using the private key (see Graunke's abstract and col. 1, lines 8-12).

The Office Action takes the position that the hardware secure module having a tamper resistant module structure recited in claim 1 is anticipated by the tamper resistant key module 52 in FIG. 2 of Graunke. FIG. 2 of Graunke is "a diagram of a trusted player having the capability to use a key mechanism without direct access to the key" (see col. 3, lines 29-31 in Graunke). Further, the Office Action asserts that the encrypted digital content E(Content) 36 in Fig. 2 corresponds to the "memory that stores the secure software", and the key module 50 in FIG. 2

corresponds to the "falsification checking unit."

FIGS. 4A and 4B in Graunke are flow diagrams illustrating the operation of a secure key distribution system, and FIG. 5 in Graunke is a diagram of the key module generation function. The Office Action alleges that the tamper resistant compiler 222 in Fig. 5 and the step 118 of checking of integrity and authenticity of manifest carried out by the key module in Fig. 4B correspond to the operations carried out by the "falsification checking unit". Further, the Office Action takes the position that the step 124 of decrypting by the key module in Fig. 4B (the decrypting after the player and the manifest have integrity and authenticity checked) corresponds to the execution of the secure software by the "processor".

However, the tamper resistant key module 52 in Fig. 2 of Graunke is not a **hardware** secure module.

FIG. 1 of Graunke is a diagram of the computer system environment. The key module 18 in Fig. 1 is "downloaded from a communications network or otherwise accessed by the storage device reader" (see col. 4, lines 46-48). Further, Graunke states that the key module 18 is preferably "provided dynamically by a content provider from a remote system over a communications network such as the Internet" (see col. 4, lines 59-61). Graunke does not clarify whether this key module 18 is equivalent to the key module 52 in Fig. 2, but in col. 7, lines 41-43, Graunke states with respect to the key module 52 that the "key module is forwarded over communications network 34 to client 32. It is a 'plug-in' to executable 44 of trusted player 42". Therefore, it appears that the key modules 18 and 52 in Graunke are software. Therefore, Graunke does not teach a "**hardware** secure module having a tamper resistant module structure and storing information related to secure software."

Furthermore, Graunke is silent with respect to the claimed falsification checking unit being "loaded on the hardware secure module", and the falsification checking unit [reading] the secure software from the memory by direct access without using an operating system" as recited in claim 1.

At least for the above reasons, independent claim 1 and claims 2-4 and 6-19 depending from claim 1 patentably distinguish over Graunke.

The Office Action fails to make a *prima facie* case that Graunke anticipates the features recited in claim 20. Graunke does not anticipates or discloses that the tamper resistant key module 52 in Fig. 2 of Graunke indicated as corresponding to the claimed "hardware secure module" reads secure software stored in a client's E(content) "using direct access method

without using an operating system." In fact Graunke in FIG. 2 and in the whole disclosure does not teach or suggest any exchange of data or any physical connection between the tamper resistant key module 52 and the E(content) 36. Moreover, the E(content) 36 is data that is decoded and not a software that can be executed. Thus, Graunke fails to anticipate or render obvious "reading secure software stored in a memory using direct access method without using an operating system, by a hardware secure module having a tamper resistant module structure which stores information related to the secure software."

Further, Graunke discloses checking the integrity and authenticity of the manifest which is "a statement of the integrity and authenticity (i.e., a signature) of the trusted player software" used in decrypting the E(content) using the private key. However, this trusted player software is not the same as the E(content) which is indicated as stored in the memory. Thus, if the E(content) in Graunke corresponds to the secure software stored in a memory, its authenticity is not verified in Graunke. On the other hand Graunke does not teach that the trusted player software is read by the tamper resistant key module 52. Thus, Applicants believe that Graunke does not anticipate or render obvious "checking falsification by a falsification checking unit that is loaded on the hardware secure module, the checking falsification being performed by comparing the secure software with the information, and determining whether the secure software is falsified based on a result of the comparison" as recited in claim 20.

Finally, since the E(content) 36 is not executable software, Graunke does not anticipate or render obvious "executing the secure software by a processor when a result of determining is that the secure software is not falsified" as recited in claim 20.

Thus, even if a person of ordinary skill in the art makes a good faith effort to use the correspondences that the Office Action indicates relative to claim 1, Graunke does not read over claim 20.

In view of the above discussion of Graunke's teachings, claim 21 and claims 22-24 and 26-39 depending from claim 21 patentably distinguish over the prior art at least because the following features recited in claim 21 are not anticipated by Graunke:

- a reading unit that reads a secure software from a memory mounted to the information reproducing apparatus by direct access without using an operating system; and
- a falsification checking unit that compares the secure software with information related to the secure software stored in the hardware secure module, and checks a falsification of the secure software based on a result of the comparison, wherein if the

result of the comparison shows that the secure software is not falsified the secure software is executed by the information reproducing apparatus.

The E(content) 36 in FIG. 2 of Graunke is not software that can be executed. The tamper resistant key module 52 in FIG. 2 of Graunke does not read the E(content) 36 by direct access without using an operating system. The tamper resistant key module 52 in FIG. 2 of Graunke does not compare the E(content) 36 with information related to the E(content) 36 stored in the resistant key module 52 in FIG. 2.

In view of the above discussion of Graunke's teachings, independent claim 40 patentably distinguishes over the prior art at least by reciting:

- reading secure software stored in a memory using a direct access method and without using an operating system, by the hardware secure module having a tamper resistant module structure storing information related to the secure software;
- checking falsification by comparing the secure software with the first information, and determining a falsification of the secure software based on a result of the comparison; and
- executing the secure software when the result of the comparison is that the secure software is not falsified.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: July 30, 2009

By: _____
Luminita A. Todor
Registration No. 57,639

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501